Marine Corps Systems Command (MARCORSYSCOM)

Requirements Analysis for Automation of the Performance Evaluation System (PES)

November 27, 2001

Agenda

Introduction	**10:00-10:15**
Review of Findings	**10:15-10:30**
PES Functional Requirements	**10:30-11:00**
Application Design Principles	**11:00-11:15**
PES Technical Requirements	**11:15-11:30**
E-Forms	**11:30-11:45**
Electronic Signatures	**11:45-12:00**
Recommended Architecture	**12:00-12:30**

Project Background

Project Background

The United States Marine Corps System Command (MARCORSYSCOM) would like to re-architect the Performance Evaluation System (PES). The PES provides for the periodic reporting, recording, and analysis of the performance and professional character of Marines in the grades of Sergeant through Major General.

MARCORSYSCOM has contracted with Gartner to develop an architecture to create an automated system with significant connectivity for forward deployed elements.

Gartner brings extensive understanding of trends in document management and scanning technologies as well as expertise in requirements analysis, office automation, and migration planning.

Project Objectives

The primary goal of this engagement is to identify the requirements and recommend an architecture for an automated PES operating environment.

In order to achieve this goal, the following supporting objectives must be met:

- Determine goals and objectives for the PES environment.

- Develop functional and technical directions to meet goals and objectives.

- Develop a technical architecture for the modernized automated PES environment.

- Provide assistance in the planning for the implementation of the strategy; including the approach to technology/vendor selection.

Approach and Methodology

Step 1. Project Initiation

– Identification of team members, roles and responsibilities, detailed project scheduling, etc.

Step 2. Information Gathering

– Approximately 10 interviews with USMC stakeholders

– Identification of USMC business drivers, technology baseline, etc.

Step 3. Research and Analysis

– Leverage Gartner research

– Leverage GartnerConsulting depth and experience.

Today

Step 4. Requirements Workshop

– Review findings

– Present high level requirements

– Recommend PES architecture

Step 5. Final Report Delivery

– Distribute final requirements report

– Distribute recommendations report

Information Gathering Process

Gartner Consulting conducted interviews to understand the current Marine performance evaluation process and the PES system supporting this process. We also conducted few focus groups with the RS and MRO communities to understand functional, process and technical requirements for an automated PES.

Results from the above interviews has enabled Gartner Consulting to:

- Develop an understanding of the current PES operating environment (As-Is).

- Identify key functions and processes of the automated PES operating environment (To-Be).

- Determine gaps in achieving the To-Be state from As-Is.

- Identify critical success factors for the automated PES operating environment.

Workshop Goals and Objectives

- Review results of information gathering sessions.

- Present and validate the high level PES functional requirements.

- Discuss the fundamental application design principles.

- Present and validate PES technical requirements.

- Present industry overview of key technologies.

- Present application development alternatives and the architectural recommendations.

The results of this workshop will assist in the development of high level PES requirements document and filling in any gaps identified in the recommended architecture.

Review of Findings

Overview of Current PES Environment

The Marine Corps Performance Evaluation System (PES) provides for the periodic reporting, recording and analysis of the performance and professional character of Marines in the grades of Sergeant through Major General.

PES supports the centralized selection, promotion and retention of the most qualified Marines of the Active and Reserve components.

The overview of PES is organized in two sections based on the current PES application:

- Front End

- Back Office

    - Scanning Operations

    - Procedure and Policies Office

Operational Overview
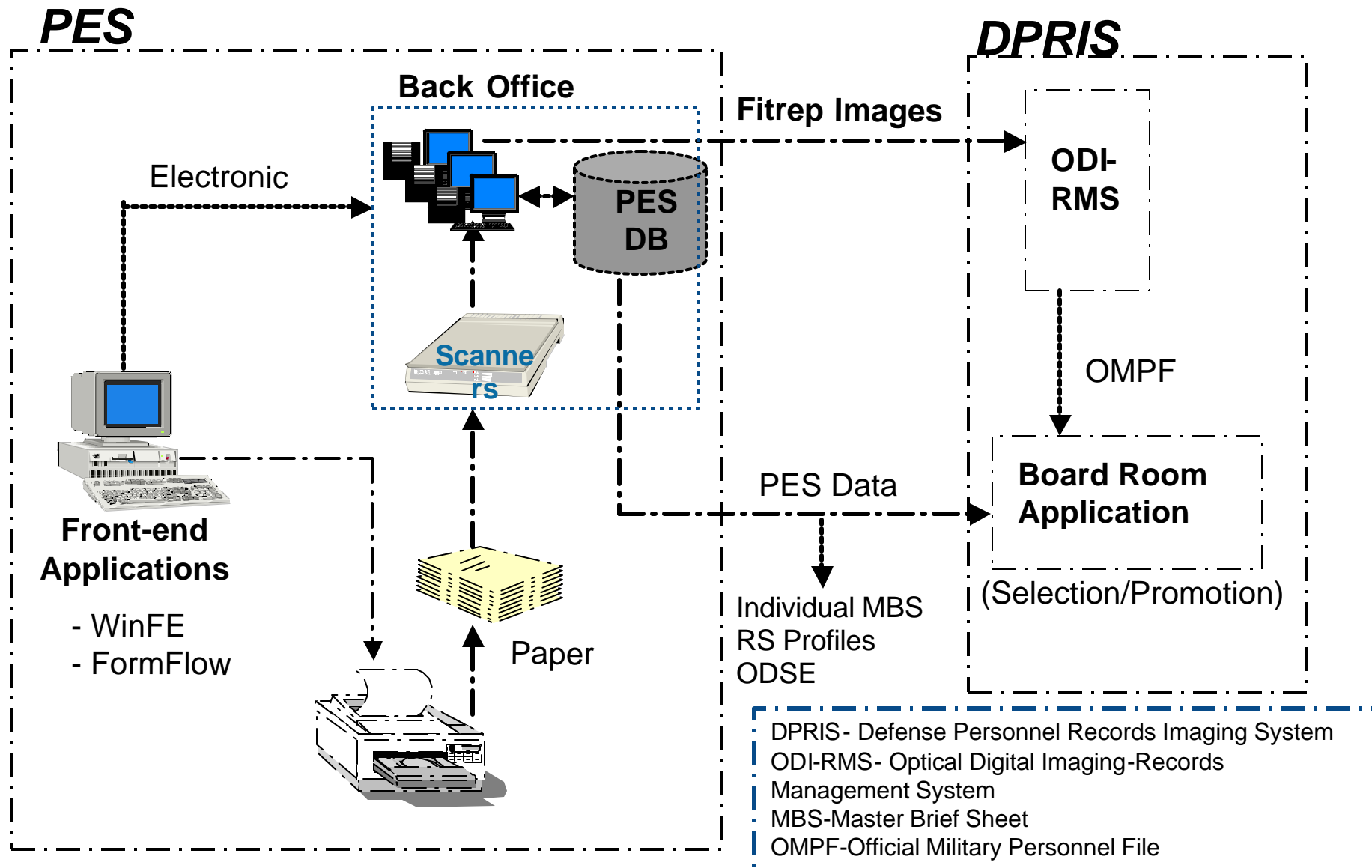
PES Overview - Front End

Performance evaluation process starts with the RS and MRO preparing MRO Worksheet (manual, paper-based process). The intent of the worksheet is to:

- Assist the RS and MRO in establishing a clear understanding of the RS' expectations.

- Means for MRO to provide his or her RS a summary of major accomplishments, awards, and other significant actions.

- Provide a tool for periodic counseling sessions to review billet descriptions.

The RS then prepares the MRO Performance Evaluation Report

- FormFlow (15%-20% of records).

- WinFE (85%-80% of records).

The RO reviews and validates the paper-based form

- Sends adverse evaluations to 3rd Action Officer.

- Ensures USMC Officer has/will review evaluation.

Following the completion of the Performance Evaluation Form

- Send completed form via postal mail to MMSB for processing.

- Represents approximately 177,000 records per year.

PES Overview: Back Office

Following receipt of Personal Evaluation Reports at MMSB

- Paper-based reports are fed by hand into scanners for input to the Back Office application.

- MMSB personnel compare the scanned Fitness Report (Fitrep) with MRO data from the operational data store (Section A information).

- Improvements in the OCR technology has brought the Fitrep review time down from 6 minutes to 2-3 minutes. The current system has achieved 87% accuracy in indexing FitReps. Indexing is the reading and matching of four key fields on each page of the 2 or 5+ page FitRep. The system does not correctly index 13% of FitReps because of discrepancies between the scanned information and the actual data and need to be manually corrected. Accuracy of fields other than indexing fields is a major problem.

- The corrected reports are APC'ed.

Procedure and Policies Office:

- Erroneous reports are reviewed by the procedure and policies office.

- Fitness Report Discrepancy sheet is sent back for appropriate action via postal mail.

PES Overview - Back Office (cont.)

There are two primary outputs from PES database

- An image file (tiff) of the Fitrep for input to the ODI RMS.

- Fitrep data for input to the PES Database.

Back Office application has been developed using the following tools:

- PowerBuilder 6.0

- Microsoft Visual Basic

- Oracle Enterprise 8.0.4

- FormFix 2.8

- Nestor Reader 5.0

- Lead Tools 10.0

- Hosted on Compaq NT server

PES Functional Requirements

Key Functional Features of Automated PES

Overall, Gartner has identified three core functional requirements in the automation of PES processes:

- Reduce/eliminate manual intervention in the overall performance evaluation process.

  – At front end, when reporting officials prepare FitRep.

  – At back end, during scanning of paper-based source document.

- Security technology and features

  – Signature requirements on the Fitrep.

  – Making sure that the person is who he/she claims to be.

- Provide automated workflow

  – Eliminate paper-based, manual processes as much as possible.

  – Reduce/eliminate discrepancies.

  – Improve review time velocity.

  – Streamline notifications for review and approvals.

PES Automation Requirements

Automate PES initiation

- Provide ability to complete MRO Worksheet and Fitrep via Web.

- No proprietary downloads for viewing forms over the Internet

- Access all PES application components through industry standard browsers

- Consistency across other web applications at Marine Corps

- Auto populate Section A information after RS initiates FitRep and allow RS to override incorrect data.

- Allow the Command to add Admin Review personnel to the routing of the MRO Worksheet/FitRep without additional signatures on the FitRep.

- Ability for MRO to view the last submitted report.

- Record and file management - assign rights to create, read, update and if required, delete Fitreps from the system.

- Enforcement of business rules inherent to current PES WinFE 3.0

- Prompt and guide reporting officials throughout the PES initiation process.

- Spell check capabilities

- Provide enhanced, secure user access

- Ability to mass produce academic FitReps.

PES Automation Requirements (cont.)

Automate PES Workflow

- Ensure timely and efficient completion of critical tasks.

- E-mail notifications to prompt actions and communicate requirements.

- Online tracking of status from the time Fitrep is created to completion.

- Retain chain of custody information to track the changes made to Fitrep (who, when, and what section).

- Clearly define the roles and responsibilities of the reporting officials for each section of the FitRep and lock all sections, except the ones the individual is expected to work on.

PES Automation Requirements (cont.)
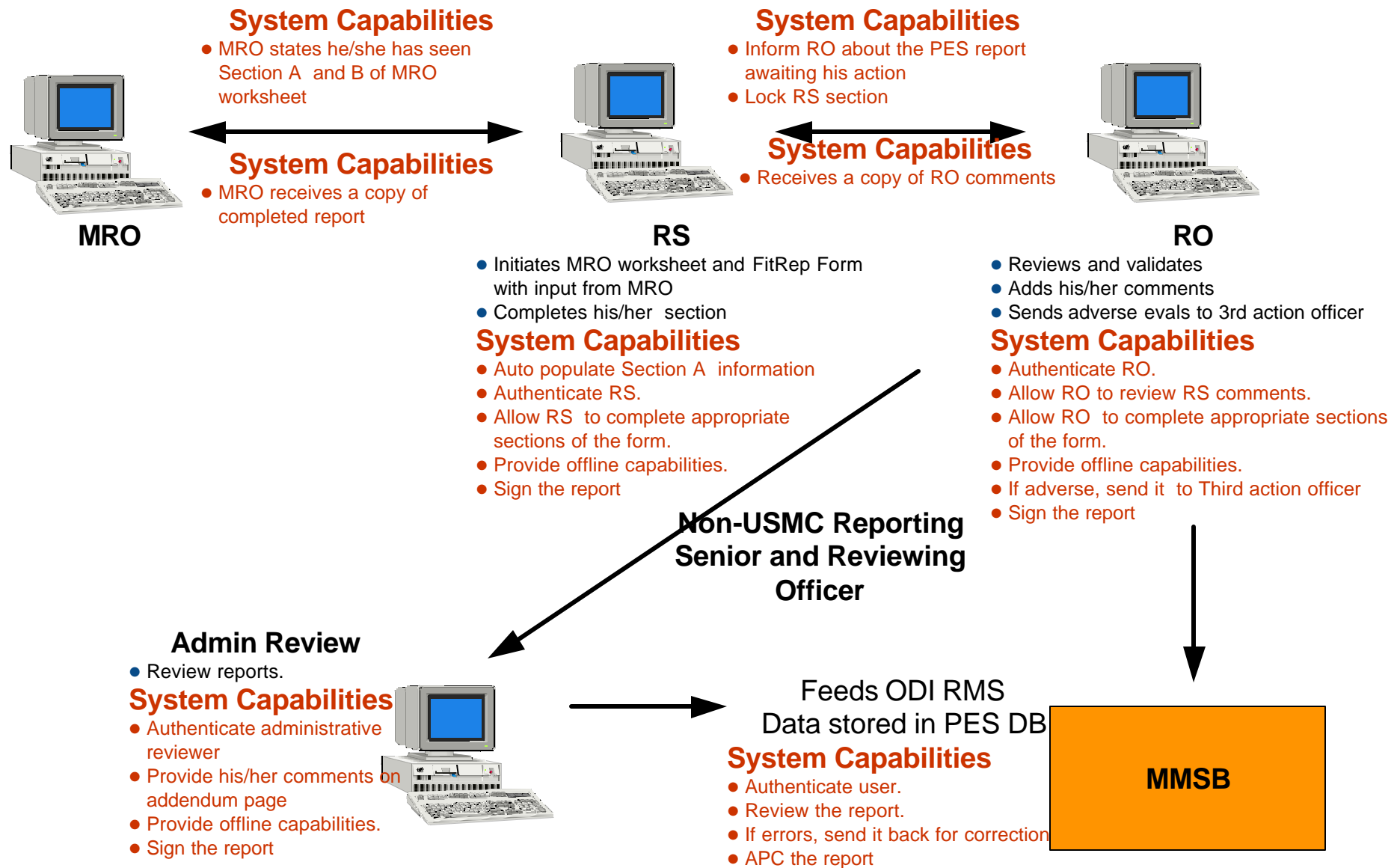
Automate PES Back Office Processing

- Continue to have ability to query previous FitReps.

- Review the report on-line.

- Identify any discrepancies and put the report back into workflow.

- Facilitate exception management to identify and locate non-compliance.

- New roles may evolve (e.g., the use of business intelligence tools to develop reports from PES DB).

PES Security Requirements

The FitRep is one of the most important reports on which a Marine's future depends. An automated PES must provide a secure environment for Marines to complete this report. The security requirements include:

- Capture signature from key personnel involved in processing and review of Fitreps:

  – Reporting officials

- Identification, authorization and authentication of users

  – Identification to gain initial access to the system.

  – Authorization of Reporting Officials to access and modify appropriate sections of the Fitrep.

  – Authentication of the user identity.

- Locking sections after receiving appropriate signatures.

  – Prevent modification to mission critical fields.

  – Protection of MRO sensitive information.

PES Functional Diagram

System Capabilities
- MRO states he/she has seen Section A and B of MRO worksheet

System Capabilities
- MRO receives a copy of completed report

MRO

System Capabilities
- Inform RO about the PES report awaiting his action
- Lock RS section

System Capabilities
- Receives a copy of RO comments

RO

RS
- Initiates MRO worksheet and FitRep Form with input from MRO
- Completes his/her section

System Capabilities
- Auto populate Section A information
- Authenticate RS.
- Allow RS to complete appropriate sections of the form.
- Provide offline capabilities.
- Sign the report

- Reviews and validates
- Adds his/her comments
- Sends adverse evals to 3rd action officer

System Capabilities
- Authenticate RO.
- Allow RO to review RS comments.
- Allow RO to complete appropriate sections of the form.
- Provide offline capabilities.
- If adverse, send it to Third action officer
- Sign the report

Non-USMC Reporting Senior and Reviewing Officer

Admin Review
- Review reports.

System Capabilities
- Authenticate administrative reviewer
- Provide his/her comments on addendum page
- Provide offline capabilities.
- Sign the report

Feeds ODI RMS
Data stored in PES DB

System Capabilities
- Authenticate user.
- Review the report.
- If errors, send it back for correction
- APC the report

MMSB

Application Design Principles

E-Business Application Deployment (2000–2005)

E-Business Applications
Deployment Trend

% of Applications of all Deployed

100%

Traditional C/S AD
• C/S 4GL
• Monolithic 3GL/4GL

> 50%

2000

Multitier Web AD
• Java IDE / 4GL
• Java Application Servers
• Application Components
• Integration With COTS
• OTM, OLTP Integration
• RAD and Systematic AD

Enterprise Application Deployment
(2000–2005)
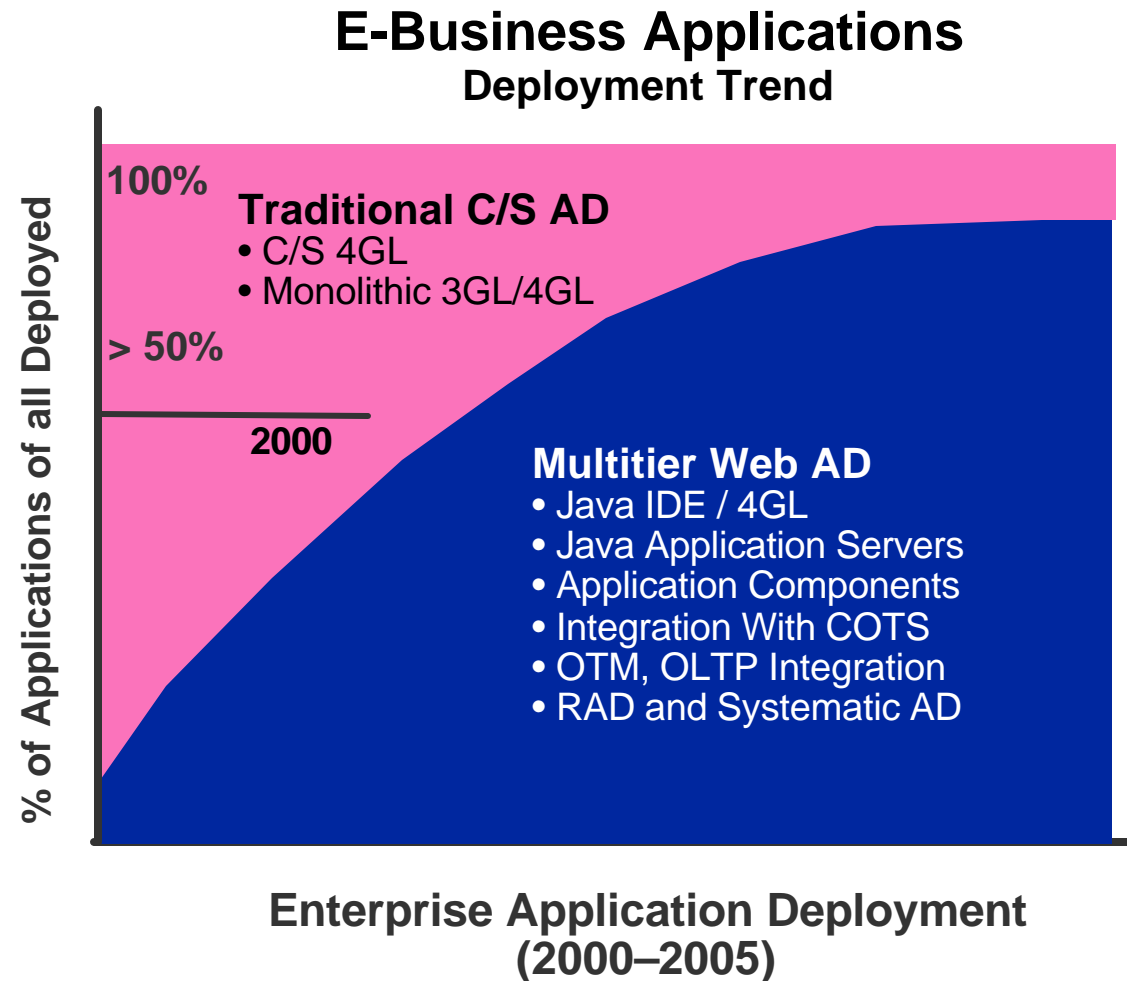
E-business applications will rely heavily on COTS-based back-office infrastructures (2000–2005)

Partitioned 3-Tier Architecture Resolves 2-Tier C/S Problems

From a software standpoint, the early C/S applications (2-Tier(a)) were monolithic executables running on a single machine—only the database lived on a server—invisibly from an application development standpoint. When the C/S applications ran into scalability and maintainability problems, they proved as intractable to change as any other legacy applications.
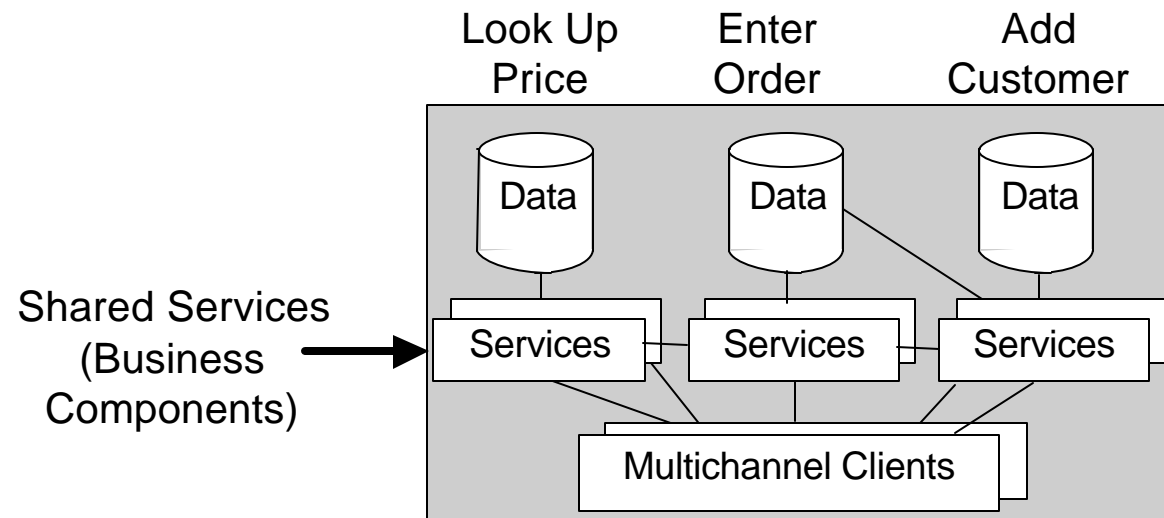
The use of stored database procedures provided some improvement, at the price of proprietary lock-in. Service-oriented architectures have emerged as superior solutions.

Fat Client 2-Tier (a)	**Plump Client 2-Tier (b)**	**Thin Client 3-Tier (a)**	**Thin Client 3-Tier (b)**
Presentation	Presentation	Presentation	Presentation
Appl. Logic	Appl. Logic		
Data Logic		Appl. Logic Data Logic	Appl. Logic
			Data Logic
DB	DB	DB	DB
	Data Logic		

←------- **Service-Oriented Arch.** -------→
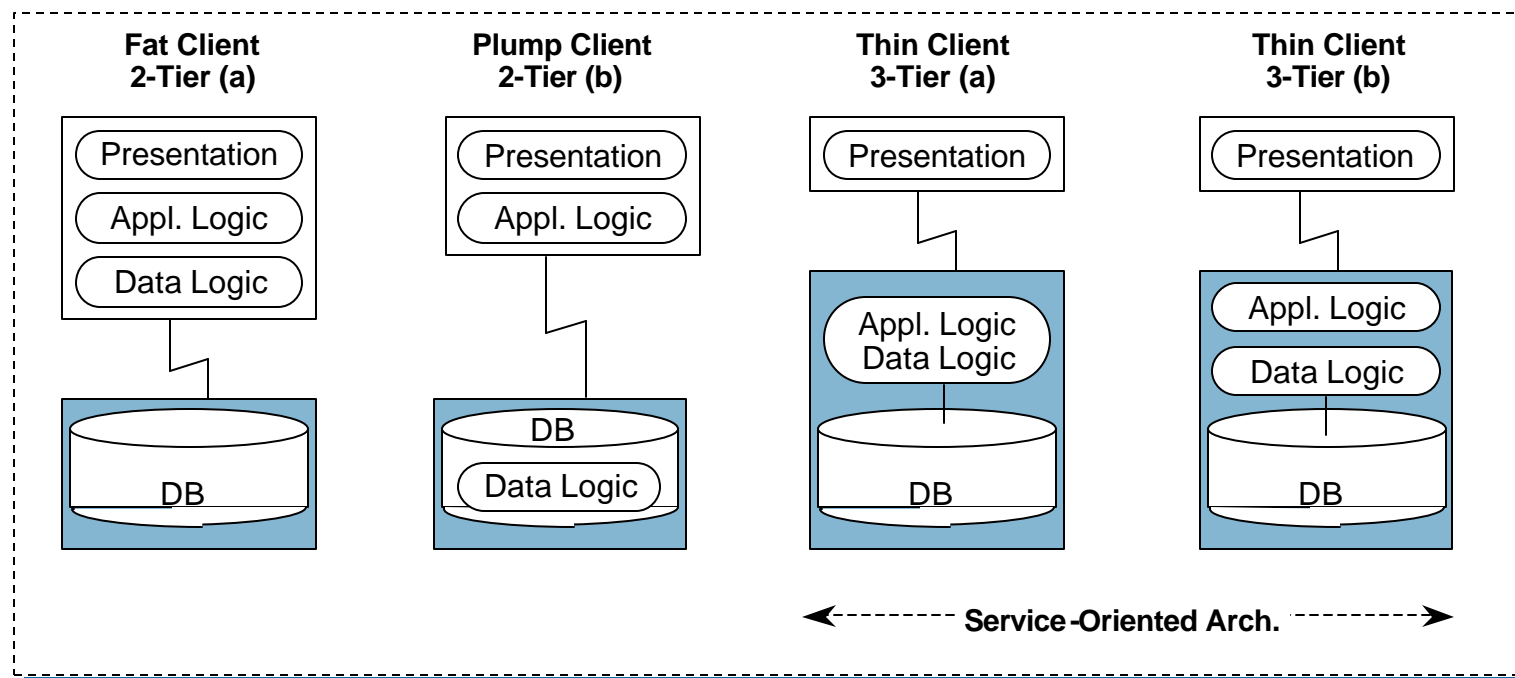
2-tier and 3-tier (partitioned) architectures

Source: Gartner

Service-Oriented Architecture

Look Up Price | Enter Order | Add Customer

Data | Data | Data

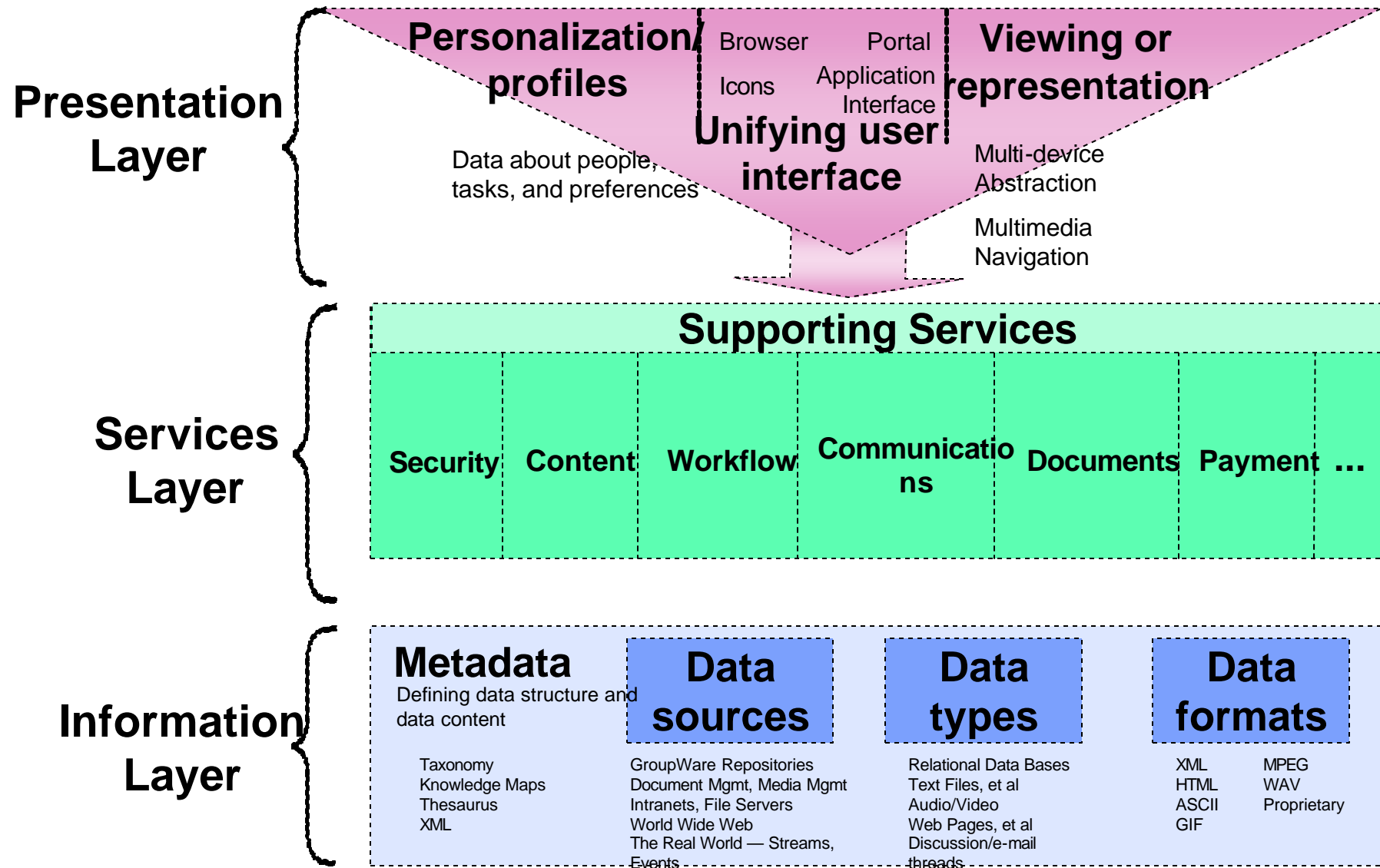Shared Services (Business Components) →

Services | Services | Services

Multichannel Clients

Service-Oriented Architecture is useful for new development that plans to incorporate previously designed business components. Business components enable heterogeneity and reuse at a coarser level of granularity than do technical software components. The software modules in a service-oriented architecture are business components.
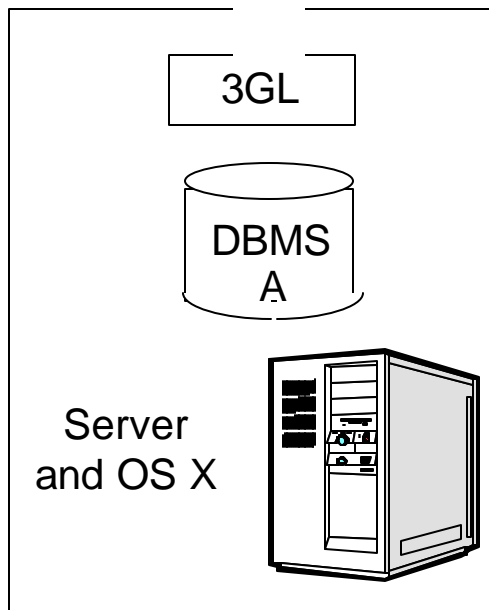
Service-oriented architectures clarify design and enable reuse by sharing logic and data among different client systems and users. The business rules and integrity checks are implemented in the black box that can be invoked by any of the participating application front ends. The logic that is unique to each client application including the presentation logic, is handled outside of the service. New clients can reuse old services, and new business processes can reuse elements of old business processes. A service addresses exactly one task and has one defined set of inputs and outputs.
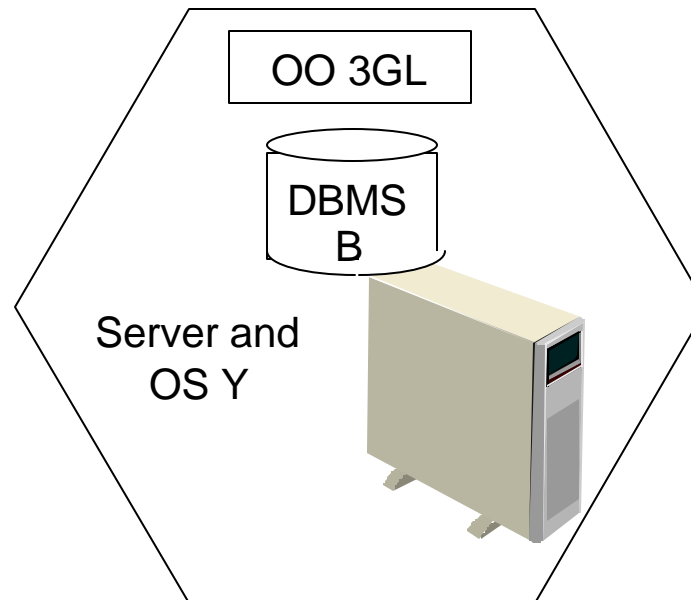
Multi-tier Application Development Paradigm

Presentation Layer

Personalization/ profiles

Browser   Portal

Icons   Application Interface

Viewing or representation

Unifying user interface

Data about people, tasks, and preferences

Multi-device Abstraction

Multimedia Navigation

Services Layer

Supporting Services

Security	Content	Workflow	Communications	Documents	Payment	…

Information Layer

Metadata
Defining data structure and data content

Data sources

Data types

Data formats

Taxonomy	GroupWare Repositories	Relational Data Bases	XML	MPEG
Knowledge Maps	Document Mgmt, Media Mgmt	Text Files, et al	HTML	WAV
Thesaurus	Intranets, File Servers	Audio/Video	ASCII	Proprietary
XML	World Wide Web	Web Pages, et al	GIF	
	The Real World — Streams, Events	Discussion/e-mail threads		

Living With Technical Heterogeneity

System A

System B

System C

3GL

DBMS A

Server and OS X

OO 3GL

DBMS B

Server and OS Y

4GL

DBMS C

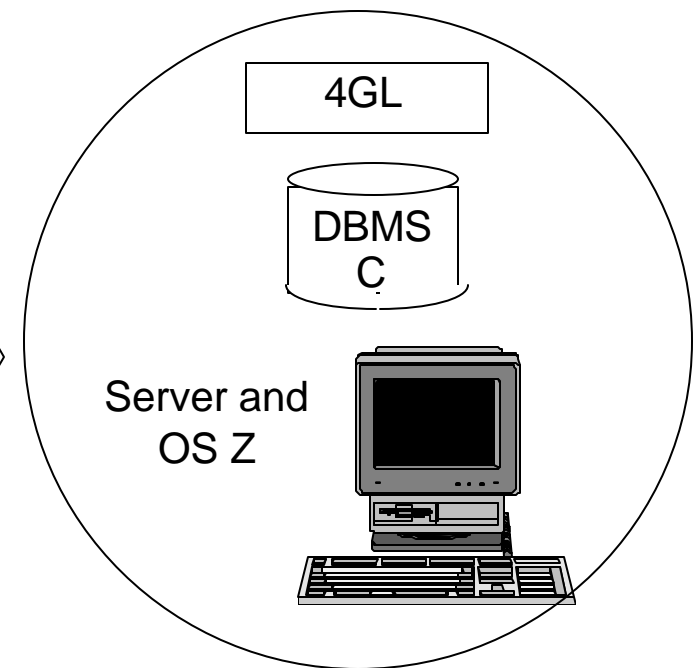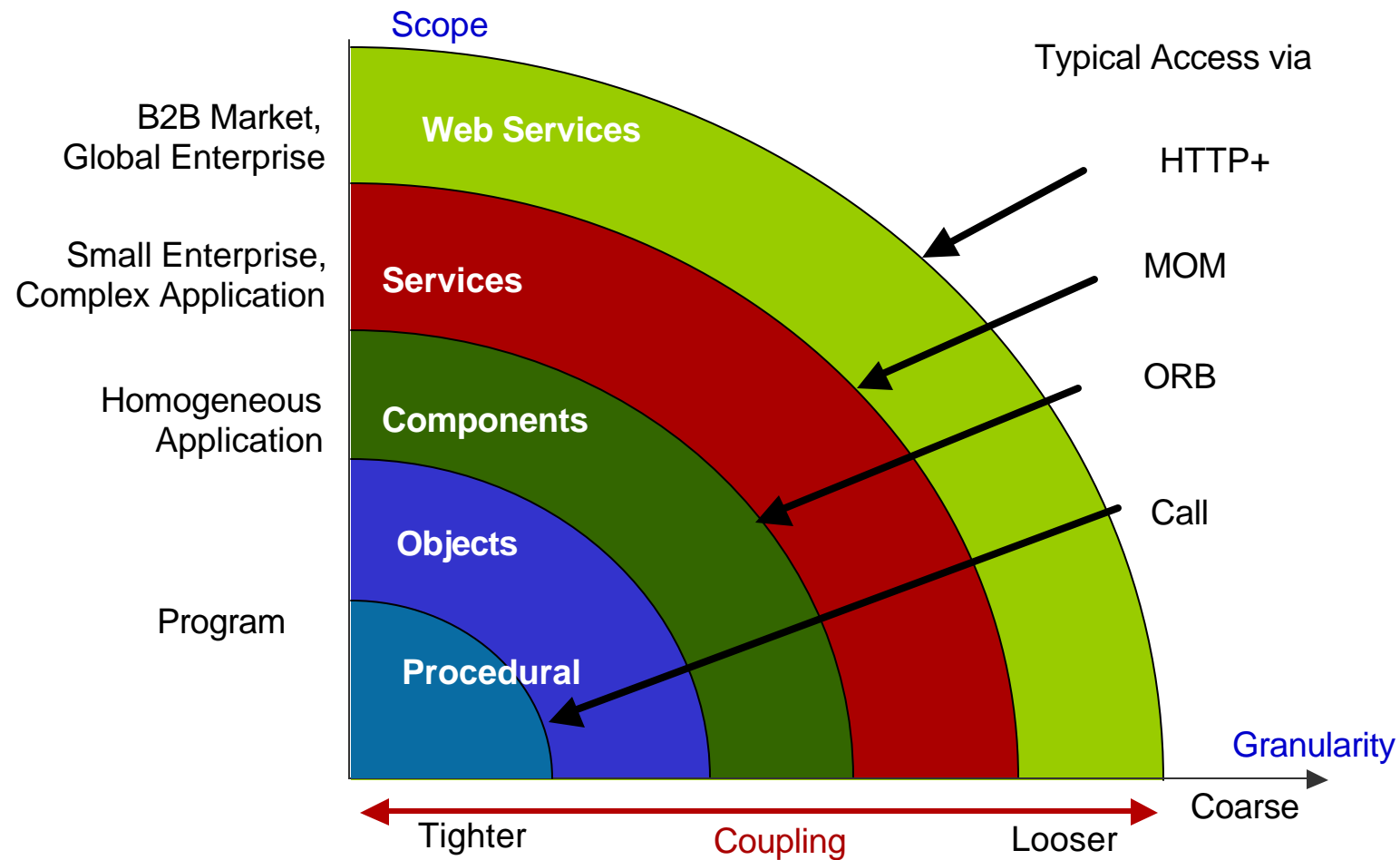Server and OS Z

The architecture must embrace heterogeneity:
- The Internet is inherently heterogeneous.
- Applications have varying heritages that also drive heterogeneity.

Integration Approaches

Best Practices in Technology Evaluation

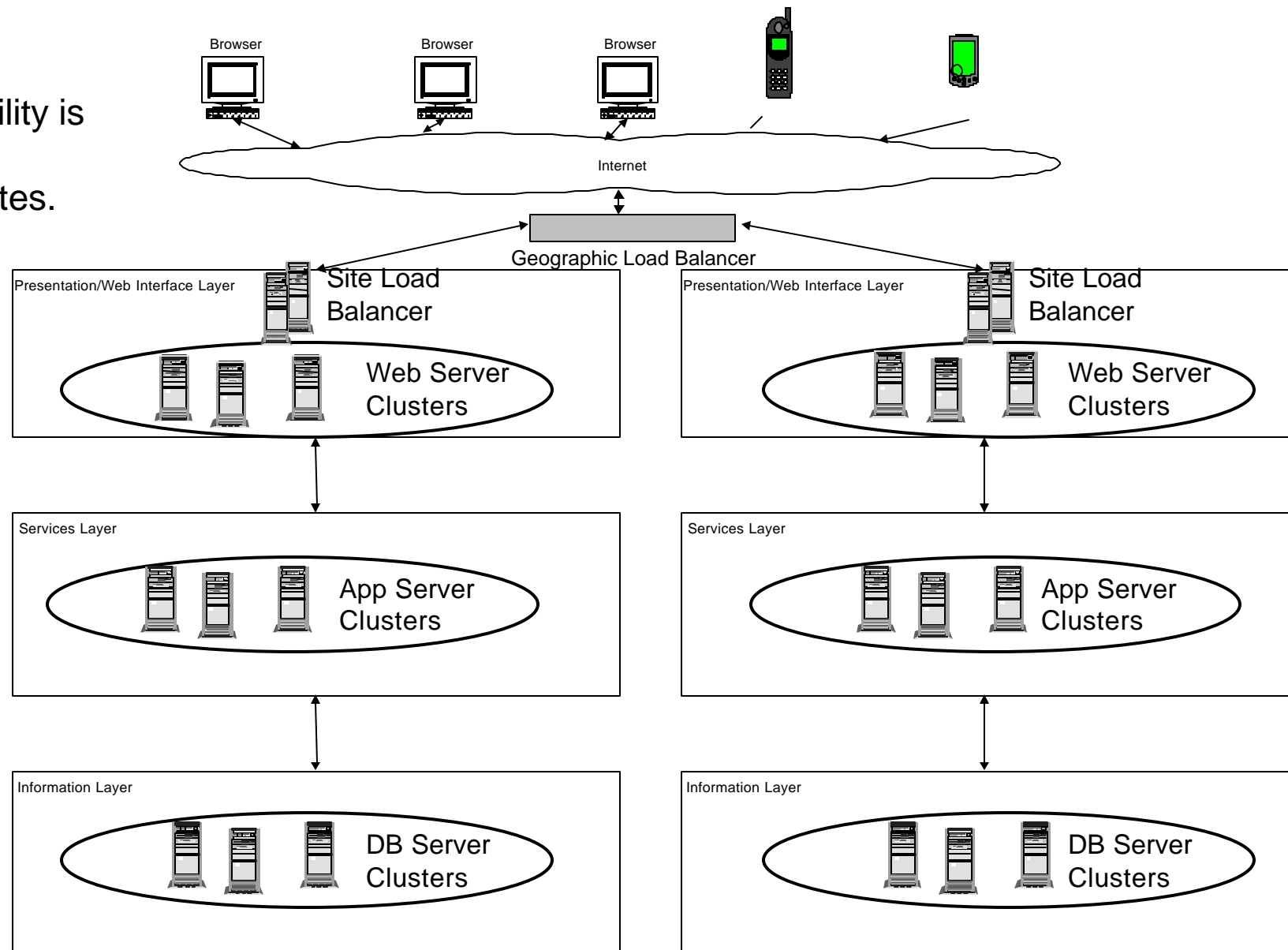|	
1. Avoid hype. Base decisions on sound information and research, not press or fashion.	*Look at what others are doing. Pay attention to successful case studies. Understand the impact of changing AD & management strategies; rationalize application development infrastructure through standardization.*
2. Money remains a driver.	*Consider the overall technology budget: Is this where you will get the biggest benefit for the dollar spent? Will the technology be cheaper next year? Are you adequately budgeting costs?*
3. Align technology with educational or business goals. Technology for its own sake is not the right approach!	*If it's neat stuff that will really get the job done, fine. Otherwise, maybe it belongs in the "hobby" category. Understand the impact to TCO.*
4. Timing is key. Jumping onto a new technological bandwagon too early can lead to costly errors, while holding off can result in lost opportunities.	*We all know that technology gets cheaper over time (consider VCRs or CD players). What we often forget is that technology <u>adoption</u> gets easier too. More people understand it, support becomes plentiful, there is more software for it, and so on … often leading to commoditization.*

High Availability Application Architecture - Strawman

High availability is achieved via redundant sites.

Browser Browser Browser

Internet

Geographic Load Balancer

Presentation/Web Interface Layer

Site Load Balancer

Web Server Clusters

Services Layer

App Server Clusters

Information Layer

DB Server Clusters

Presentation/Web Interface Layer

Site Load Balancer

Web Server Clusters

Services Layer

App Server Clusters

Information Layer

DB Server Clusters

Fundamental Design Principles

- Run the application in a browser utilizing a thin-client architecture; separation of presentation logic from application (business) and data access logic

- Use Three Tier/N-Tier Architecture

- Utilize Service-Oriented Architecture

- Prefer loose coupling

- Adhere to technology adoption best practices

- Prepare to support heterogeneity

- Provide high availability

PES Technical Requirements

PES Technical Requirements

Based on the discussions with PES stakeholders, results of focus groups and current technology trends, Gartner has identified the following technical requirements for automated Performance Evaluation System.

Client Requirements

- Thin client approach

- Complete functionality using industry standard browser (Netscape and IE) technology (constrained by DoD/DoN/MC/NMCI implementations)

- Platform independent

- Device independent (support kiosks, if required)

- No proprietary downloads for viewing forms over the Internet

PES Technical Requirements

Services layer requirements

- Supports workflow engine and/or business process manager.

- Provides workflow integration with existing e-mail systems.

- Supports application integration using industry standards (e.g., XML).

- Manages database connections.

- Provides access to PES DB.

- Provides access to operational data store (ODSE) for Section A information.

- Import reporting hierarchy information from HR systems or LDAP directory.

- Provide Fitrep images (tiff files) to Optical Digital Imaging - Records Management System (ODI-RMS).

- Supports standard database access protocols like ODBC and JDBC.

- Integrate with DoD Common Access Card (CAC).

PES Technical Requirements (Cont'd)

Security Requirements

- Comply with Federal Electronic Signature Act

- Comply with DoD PKI policy

- Interoperate with DoD Common Access Card (CAC) or other DoD approved hard token

- Comply with DoD Class 3 PKI Public Key-Enabled Application requirements

PES Technical Requirements

Data Layer Requirements

- Leverages PES DB structures, schema, records, etc. with minimal changes.

- Store and maintain data required to support any digital signatures

- Scalable database solution to support more than 175,000 reports per year.

- Comply with Marine Corp data archival policy.

- Provide inputs to generate Master Brief Sheets (MBS).

- Provide inputs to Operational Data Store Enterprise (ODSE) server.

- Database should be accessible to conduct statistical analysis.

Decision Points

Based on the PES technical requirements, following are the key technology decision points:

1. Application server platform

2. Web Server

3. Programming language and application development environment

4. Database (reuse current PES DB Oracle database)

5. Middleware & Protocols

6. Workflow/Business Process Management application engines

E-Forms

Evolution of E-forms

	Strengths	**Weaknesses**
Paper Forms	Simple for users, easy to mark up	Inflexible, error-prone, and expensive to store, process and access forms
C/S GUI-Based Forms	Sophisticated client-based edits, stateful interaction, fast	Difficult to roll out client software
First-Generation Web-Based E-Forms (HTML)	Easy to deploy via browsers, can be ASP hosted	Lack of state
New Generation Web-Based E-Forms (XML)	Sophisticated edits, stateful interaction easy to deploy	Performance and bandwidth requirements

E-Forms - What to Look For

Some key features that an enterprise considering E-forms should look for are:

- **XML Support:** The major benefit of XML-based E-forms over traditional systems is that it provides information (metadata) about data and therefore many different classes of applications will be able to share an XML-based E-form components. Most of the vendors claim XML as their standard, but XML is just a syntax; how the information is formatted is up to the vendor. In addition, XML does not include any capability for version control or security. Consequently, all the vendors are developing their own standards (e.g., XFDL from PureEdge, XFA from JetForm, and BizTalk from Microsoft) and positioning them as marketplace "standards". .

- **Workflow**: A tool for structuring business process automation and handling the interrelationships between the components of a business process— participants, procedures, information, tasks, and management. Many E-forms vendors have recently extended their workflow capabilities to provide internal and external workflow.

- **Electronic Signatures**: Most E-form products provide built-in digital signature capabilities that may not be adequate for all applications. A built-in E-form digital signature service may use an enterprise's E-mail system's administration and security features to identify the signer. However, because an internal digital signature system cannot easily and absolutely "vouch" for the signer's identity, some E-form vendors offer integration with PKI products.

E-Forms Marketplace

Three products are leading the way in offering Web-enabled electronic forms. These vendors are:

E-Forms Vendors/Products	
Tier 1 Vendors/Products	**Tier 2 Vendors/Products**
Accelio (JetForm) / Capture, Integrate, Present	MMA (Multimedia Abacus)
Shana / Informed, Aurora	Cardiff / PDF Forms, Audience One, LiquidOffice
PureEdge Solutions	Microsoft / Exchange, Outlook, Biz Talk Repository

E-Forms Marketplace - Accelio

- A software and services company, Accelio (JetForm) has dominated the e-forms business and has the largest share of end users using its electronic forms creation and routing system.

- In business since 1982, Accelio has a global presence, with more than 8.5 million users worldwide.

- Vertical industry focus:

  - Financial services

  - Banking

  - Public sector

  - Utilities

- Internet posed a challenge for JetForm, but with recent offerings it has repositioned its business to be Internet centric and has developed its own XML syntax, XFA.

- Provides lock form data capabilities with digital signatures.

- Integrates with Entrust and Sonera security products.

E-Forms Marketplace - PureEdge

- Formerly UWI.com, PureEdge, has been the technology leader in the E-forms industry, it has developed a series of extensions to XML, named XFDL, that are designed to manage security and other aspects of e-forms, which the XML standards did not address.

- Vertical industry expertise includes:

  - Government

  - Healthcare

  - Financial Services

- Supports electronic signatures from various security vendors including RSA, Baltimore and Entrust.

- SEC, DoD and U.S. Patent Office have been some of the recent big wins.
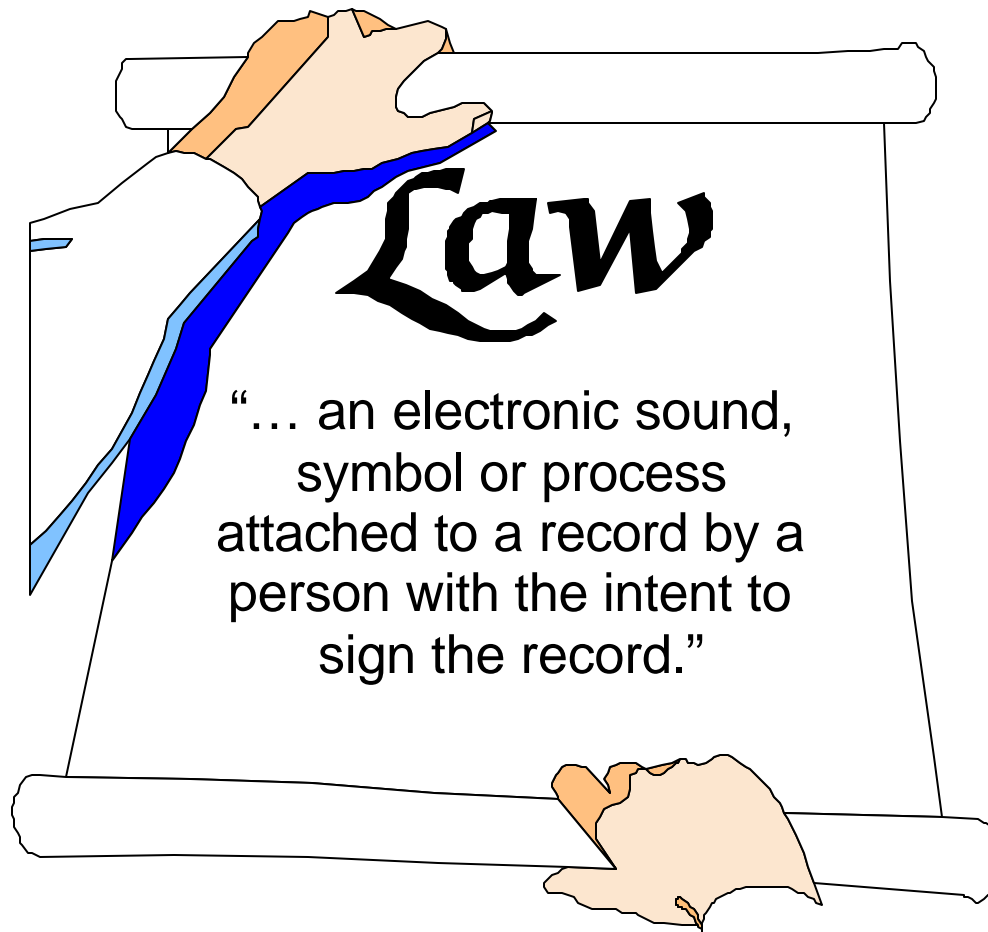
E-Forms Marketplace - Shana

- Shana is a privately owned corporation founded in 1985. They were among the earliest developers of e-Forms software.

- Shana's Informed provides an e-form portal with the standard set of design, entry, processing and workflow modules.

- Its XML compliance is based on Xforms.

- Shana's integrated e-Forms solutions are used by more than two million people around the world. Its customer base spans many industries, notably

  - Aerospace

  - Public Sector

- The software supports Entrust digital signatures and lets users route forms over existing mail systems.

Summary - E-forms

- E-forms provide an efficient solution for PES automation at all stages including fitness report preparation, submission and processing.

- E-forms technology has matured in the past few years and is ready for mass adoption.

- Leading E-form vendors meet all critical functional requirements for Automated PES, including:

    - Automated Workflow

    - Digital Signature

    - Lock form data

Electronic Signatures

Electronic Signatures in Global and National Commerce Act (E-Sign)

"… an electronic sound, symbol or process attached to a record by a person with the intent to sign the record."
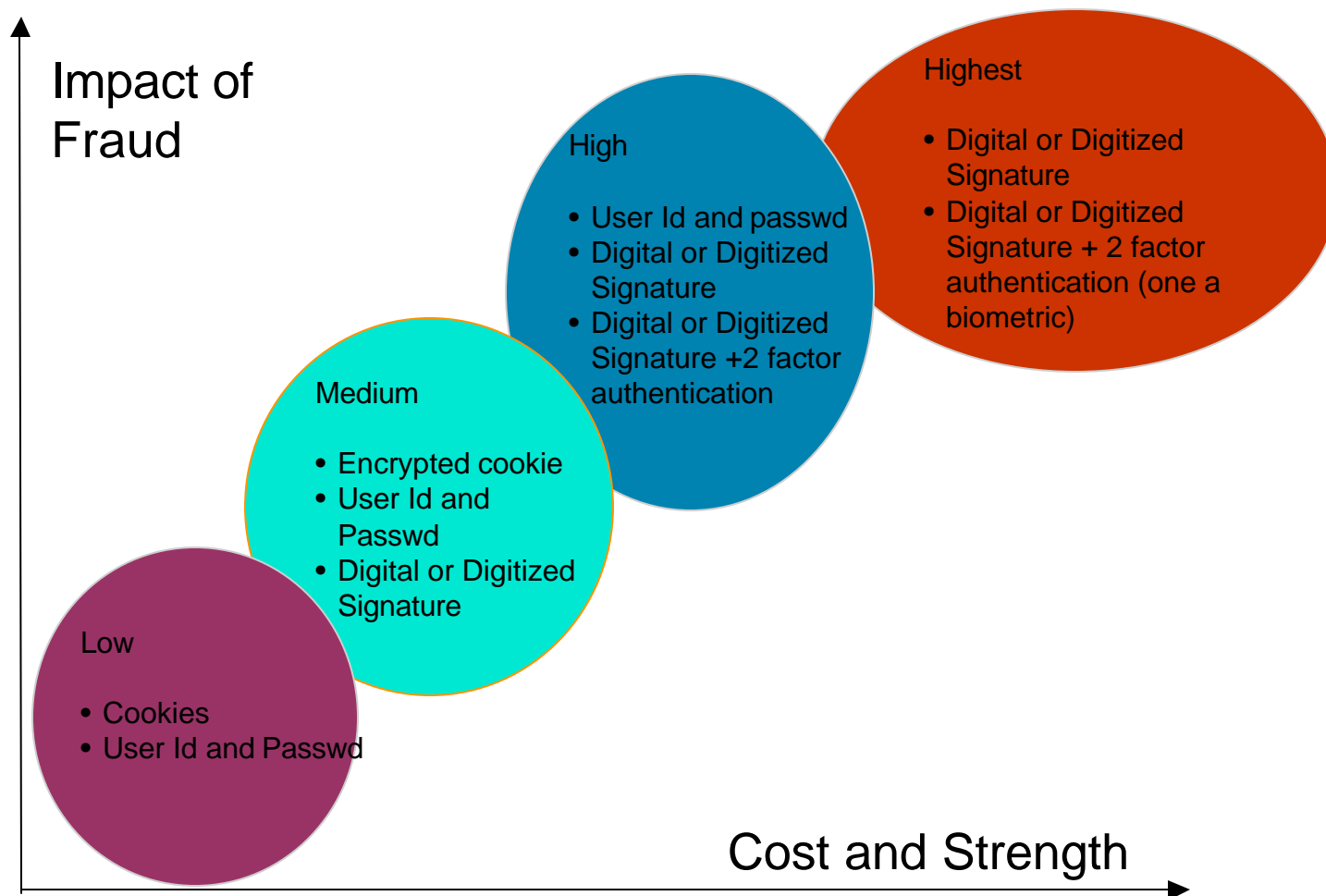
- E-Sign is technology-neutral, which is both good and bad news. *The good news:* The law is less likely to become dated. *The bad news:* It is up to organizations and industries to choose a technology and continue until the inevitable court tests.

- The passage of the law gives consistency of e-signature laws throughout the United States, enabling e-business to proceed unimpeded across state lines.

Some Concerns About E-Sign

- No distinction between digital and "digitized" signatures

- Fails to associate security levels with specific signature technologies

- Often confused with other government directives

- No procedures for testing in court.

E-Sign Act's definition of e-signature is quite generic and broad, it covers any unique information serving as a signature that can be digitized and read on a computer.

Approaches to Online Authentication

Impact of Fraud (vertical axis) vs Cost and Strength (horizontal axis)

Low
- Cookies
- User Id and Passwd

Medium
- Encrypted cookie
- User Id and Passwd
- Digital or Digitized Signature

High
- User Id and passwd
- Digital or Digitized Signature
- Digital or Digitized Signature +2 factor authentication

Highest
- Digital or Digitized Signature
- Digital or Digitized Signature + 2 factor authentication (one a biometric)

Authentication vs. Identification and Authorization

Who are you?	Requires **identification**, to gain initial access to the system.	Usually established by a user identifier (user ID) or user name.
What are you allowed to do?	Requires **authorization,** a process which determines what resources you may access and what you may do with them.	Established by permissions or access rights — such as read, write and update — associated directly or indirectly with the user ID (or assigned role) and with the electronic content.
Prove you are who you say you are	Requires **authentication**, in which you offer proofs and credentials to verify your identity. Also called **verification**.	Usually established by a number of "proof of identity" requirements, of which the password is merely the simplest. Often requires a combination of more than one means of proof.

PKI Based Digital Signature Advantages

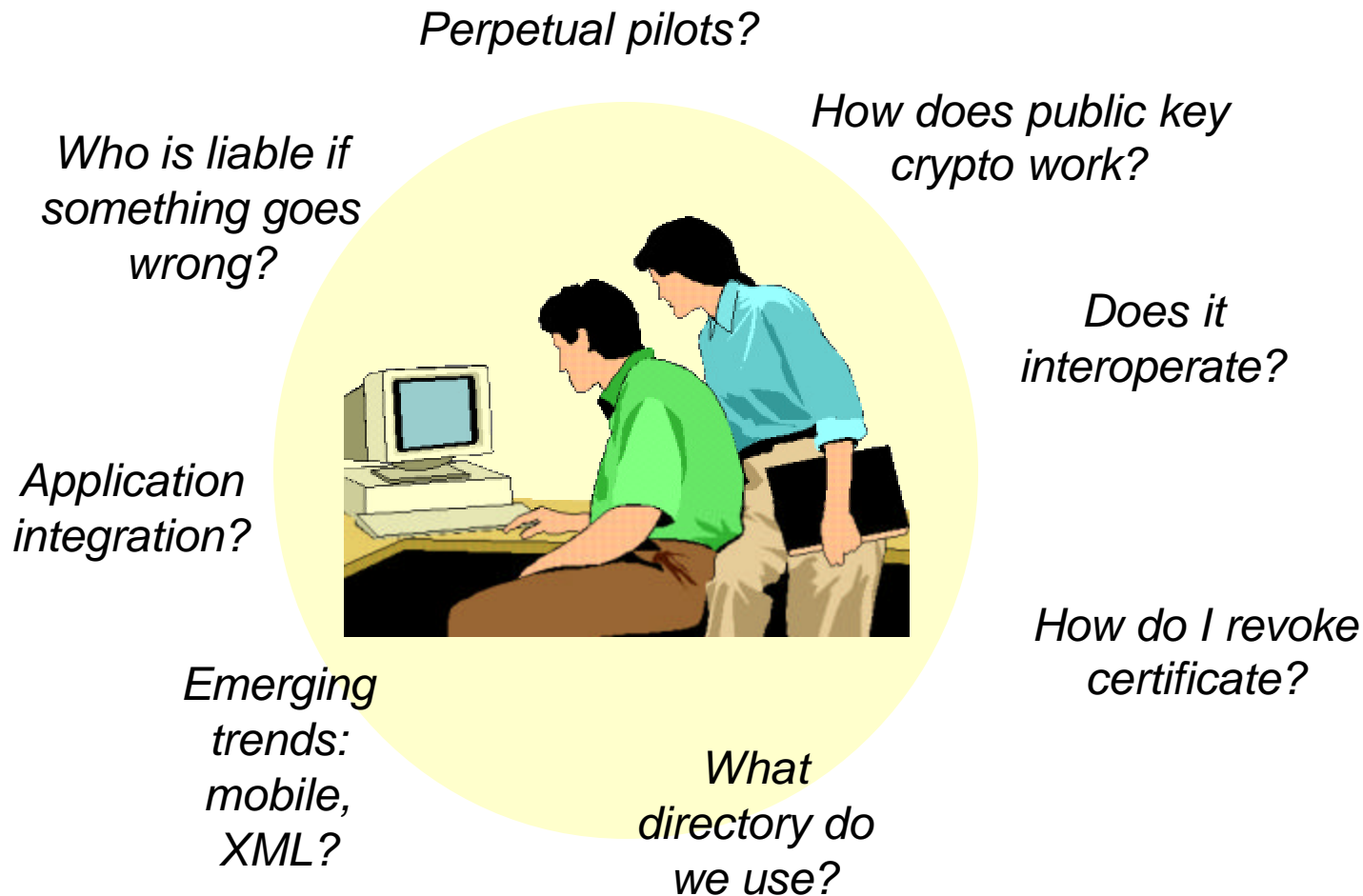| Security Need	Definition	PKI Advantage
Integrity	Integrity is the assurance that the message is whole, complete, and not changed in transmission.	As digital signatures are created from a hash of the message content, the content is protected. Any alteration in the message would invalidate the signature.
Nonrepudiation	A legal issue rather than a security issue, nonrepudiation means that neither party to the transaction can later claim that the transaction did not take place or that the signature is not valid.	The digital signature is encrypted with the signer's private key, binding the signer to the document. Use of time stamp further reinforces nonrepudiation.
Confidentiality	Confidentiality means that access to the content of the document is limited to authorized persons, thus eliminating the possibility for disclosure or theft of information or signatures.	Many messages and contracts are sent "in the clear," the important issues being a valid signature and an unchanged document. However, in the event of sensitive or proprietary information, PKC or other encryption can be incorporated into the digital signature process, allowing the entire message to be encrypted.
Authentication	Authentication provides the assurance that the person affixing a signature to an electronic document is, indeed, who he or she claims to be.	The *public key certificate*— which is signed with the private key of a trusted third party called a *certification authority*— binds the key pair to the sender.

Is PKI Really for Everyone?

Simply put, the higher the degree of certainty needed in the authentication, the more complex and expensive the infrastructure required to implement it.

To proceed with any PKI or digital signature project, it is necessary to determine:

- The degree to which transactions contain sensitive information and are subject to fraud

- If the enterprise is "ready" for PKI; has a well formed information security infrastructure; high level of knowledge of information security and encryption.

- Risk assessment of legal ramifications if transaction is compromised.

- If verified identity of individual or business entity is essential — verification must be strong enough for effective nonrepudiation services (i.e., authentication credentials under sole control of individual user).

PKI is handy, but not essential for identification, authentication and authorization processes.

PKI Issues

Perpetual pilots?

How does public key crypto work?

Who is liable if something goes wrong?

Does it interoperate?

Application integration?

How do I revoke certificate?

Emerging trends: mobile, XML?

What directory do we use?

The "unresolved issues" associated with PKI are insufficient reasons to inhibit enterprises from PKI initiatives if there are compelling, beneficial applications and services present.

DOD PKI Initiative

To address security requirements, DOD developed a Public Key Infrastructure (PKI) to provide products and services that enhance security of networked information systems and facilitate digital signatures. Key components of the PKI include hardware and software that:

- Issue and manage X.509 certificates.

- Identify and bind the client to a unique public/private key pair for cryptographic purposes.

- Provide directory services for storage and archiving of certificates and certificate revocation lists.

DOD PKI initiative is currently in its initial stages. It is expanding rapidly with thousands of certificates being issued every month.

PKI at Marine Corps

- Marine Corps has issued approximately 5000 certificates.

- Only a fraction of them are actually being used.

- Marine Corps plan to issue all certificates on Common Access Card (CAC)

- DOD has set a deadline of Oct 2002 to issue PKI certificates to everybody, this date is expected to slide to early 2003.

- At present, no commercial PKI vendor meets all DOD requirements.

- Only one production application uses DOD PKI at Marine Corps, the application is used by over 400 Office of Government Ethics users.

Key Issues Regarding Digital Signature Usage for PES

- DOD PKI initiative is expanding rapidly.

- PKI implementations for individual applications are prohibitively expensive. PES development team should work closely with Marine Corp PKI program manager to leverage enterprise wide investment in PKI.

- PES might be the first enterprise wide application to use DoD PKI at Marine Corps, therefore PES implementation plans must include mitigation strategies for PKI risks including delay in DOD PKI rollout.

- While PKI based solutions provide the strongest authentication and authorization capabilities, it is not essential for identification, authentication and authorization processes.

- PES must select E-forms vendor that can both:

  - Demonstrate capability to integrate with DoD PKI, and

  - Provide other (non-PKI-based) solutions for authentication and authorization.

Recommended Architecture
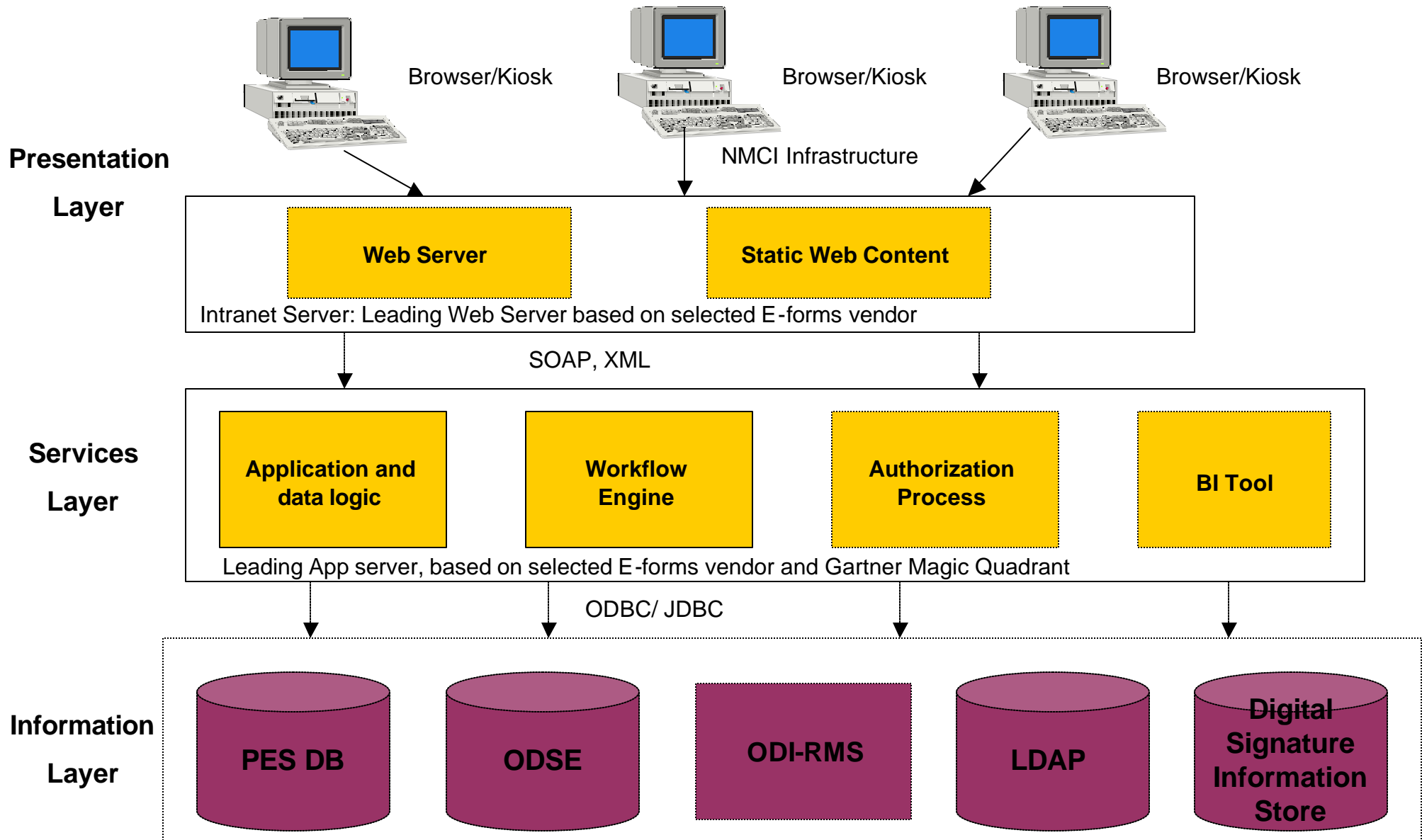
Analysis of Alternatives Considered

Approach	Strengths	Weaknesses
Commercial of the shelf solution (COTS) Performance evaluation system	• Marine Corps will be able to leverage vendor investments in maintaining the product and can rely on vendor to introduce state-of-the-art features and business process best practices.	• No large COTS vendor in this field. • Performance evaluation is often unique to enterprises therefore most large organizations have internally developed their performance evaluation system.
Custom Application Development	• Large numbers of organizations have developed homegrown Internet forms applications to gather information - using HTML, CGI scripting, Visual Basic. • Allows flexibility; meets needs exactly. • Often cheaper to develop.	• Workflow is a big challenge in this approach. • Must be integrated with enterprise security solutions. • Significant application maintenance costs.
Custom Development using E-forms Components	Electronic forms software provides four elements that help streamline processes: • Graphical workflow tools that let you map out the simplest and cleanest way to get a job done • Standard formats such as XML that let the form data interact with other applications. • A user interface that mimics the forms people normally fill out to initiate a workflow • Digital signatures that keep approvals and processes legal, even without handwritten signatures.	• Vendors must be carefully evaluated. • License costs make the solution expensive.

Gartner recommends using Custom Development with E-forms for automating PES.

Candidates —Choices Are Semi-independent

Element	Choice 1	Choice 2	Choice 3
Application Server OS	NT	UNIX	LINUX
GUI Languages	HTML/ XML/ Java	HTML/ XML/ VB	
Server Programming Language	Visual Basic	Java	
Database	Oracle		
AD Environment	AD Environment provided by selected E-forms vendor.		
Web Server	Web Server supported by selected E-forms vendor.		
Application Server	Application server supported by selected E-forms vendor.	Gartner considers BEA, IBM, Microsoft, Sun/iPlanet as leading app. Servers.	

Overall Architecture - Intranet based PES

Presentation Layer

Browser/Kiosk   Browser/Kiosk   Browser/Kiosk

NMCI Infrastructure

Web Server	Static Web Content

Intranet Server: Leading Web Server based on selected E-forms vendor

SOAP, XML

Services Layer

Application and data logic	Workflow Engine	Authorization Process	BI Tool

Leading App server, based on selected E-forms vendor and Gartner Magic Quadrant

ODBC/ JDBC

Information Layer

PES DB	ODSE	ODI-RMS	LDAP	Digital Signature Information Store

Recommended Implementation Approach

MARCORSYSCOM must evaluate the ability of the leading E-forms vendors (Accelio, PureEdge, Shana) to meet PES functional and technical requirements through pilot implementation.

Pilot must demonstrate:

- Ability to meet key functional requirements

- Ability to automate workflow

- Ability to authenticate the users

- Ability to work within NMCI infrastructure

- Vision to meet DoD PKI policy

Recommended Implementation Approach (Cont'd)

Description of Major Tasks	Comment
Early PES Redevelopment (2-3 months)	
Develop detailed functional and technical requirements	Complete documentation, including identification of interfaces.
Database modifications	Leverage existing PES DB.
Application Design	Continue design by flushing out methods for each busine object.
Begin PES redevelopment to the 3-tier architecture: 1. Presentation Layer (Forms) 2. Services Layer 3. Information Layer	Development of selected forms and processes.
Develop internal and external interfaces	Extensively test the interfaces and any impact on other systems
Early QA	Examine the processes and results, test the initial code. Implement corrective actions as appropriate.
PES Automation: Phase One (8-10 months)	
Development Phase One	Intranet based PES system; build should be limited by tir not by critical functionality.
QA and testing for Phase One	
Refine processes as required	Development processes must be well established by the end of Phase One.
PES Automation: Phase Two (15-18 months)	
Development of Phase two	Internet based Automated PES system
BI Tool Selection	
Consider deploying BI tool against current databases or a data mart.	There is a demand for user-friendly reporting and analys
QA and testing for Phase Two	

Note: Timeline represents months taken after pilot and vendor selection

Next Steps

Next Steps

Based on the comments and suggestions provided during this workshop, Gartner will:

- Consolidate the functional and technical requirements of PES.

- Make changes to this workbook.

- Develop high level functional and technical requirements document.

- Provide copies of requirements document and updated workbook to MARCORSYSCOM.